UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,375	08/20/2003	Keith Ballinger	13768.454	7425

47973 7590 08/13/2008

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
SAN JUAN, MARTINJERIKO P	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/645,375	BALLINGER ET AL.	
	Examiner	Art Unit	
	MARTIN JERIKO P. SAN JUAN	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-9,11-14,17-24,26-29 and 32-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 6-9, 11-14, 17-24, 26-29, and 32-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a response to a Request for Continued Examination filed on May 16, 2008.

Claims 1-3, 6-9, 11-14, 17-24, 26-29, and 32-36 are currently pending.

Response to Arguments

1. Applicant's arguments, see Remarks and Amendments, filed May 16, 2008, with respect to the rejection(s) of claim(s) 1-3, 5-7, and 14 under 35 USC 102(b), and 29 under 35 USC 112(1st par) have been fully considered and are persuasive. Therefore, the rejections have been withdrawn.

2. New ground(s) of rejections are being made with respect to prior art by Kent et al. [NPL 1998], in view of Fieres et al. [US 6178504 B1], and de Jong et al. [US 2004/0054628 A1].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

1. Claims 1-3, 6-9, 11-13, 17-24, 26-29, and 33-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kent et al. [NPL 1998], and further in view of Fieres et al. [US 6178504 B1], and de Jong et al. [US 2004/0054628 A1].

Regarding claim 1, Kent teaches in a computerized network environment including two or more computer systems sending messages through a network [Kent Pg 1, Sec 1, Par 1], a method of receiving using custom security tokens [Kent Pg 1, Sec 1, Par 2], the method comprising: an act of receiving a message, the message comprising a non serialized portion [Kent Pg 7, Sec 3.1 --IP header, routing fragment information header, security header (ESP) read on non-serialized portion.], wherein the non-serialized portion comprises destination information, such that intermediate computer systems that relay the message to a receiving computer system do not need to deserialize portions of the message to identify an intended recipient of the message [Kent Pg 7, Sec 3.1 --IP header, routing fragment information header, security header (ESP) read on non-serialized portion.]; an act of identifying the one or more security tokens in the received message [Kent Pg 12, Sec 3.4.2 --Parsing the packet for processing data extracted from various packet headers reads on "an act of identifying."] that has at least a portion that has been encrypted using the one or more security tokens [Kent Pg 10, Sec 3.2.1 --Data payload is encrypted using information from ESP.], and a value type corresponding with each identified security token [Kent Pg 13, Sec 3.4.2 –Security

association is a value type.]; and an act of decrypting an encrypted portion of the received message [Kent Pg 16, Sec 3.4.5] and accessing the received message based at least in part on the raw data received from the at least one identified security token [Kent Pg 16, Sec 3.4.5 -Information from ESP is used to decrypt data payload of message packet.].

Kent does not teach an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access, wherein the stored value type comprises a custom program classes including a collection of executable instructions for data handling, including instructions that tell a computer system how to read data associated with a specific security token that was created using the value type. Kent also does not teach an act of receiving data from the at least one identified security token into the stored value type that has been matched.

Fieres teaches an act of generating one or more security tokens [Fieres 6: 29-30 -- application certificate reads on tokens] using one or more corresponding value types [Fieres 6: 29-30 --COS reads on value types.], an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access, wherein the stored value type comprises a custom program classes including a collection of executable instructions for data handling [Fieres 5: 17-35 --Each type of COS has a particular set of cryptographic functions and supporting library programs for handling data in a request.], including

instructions that tell a computer system how to read data associated with a specific security token that was created using a specific value type [Fieres 7: 66 – 8: 3 --The cryptographic functions and its other supporting library of programs include instructions that tell a computer how to read/compute challenge data (payload data) of a request associated with a specific security token with a corresponding COS.], and an act of receiving data from the at least one identified security token into the stored value type that has been matched [Fieres 14: 29-55 --COS attributes are extracted and used by the stored COS type program/functions to govern its operation.].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Kent by customizing security using one or more corresponding value types as taught by Fieres. The suggestion/motivation for combining would have been to allow for compliance in the distribution and exercise of various cryptographic capabilities under the control of a policy using security tokens [Fieres 2: 47-63]. Fieres is analagous art because it is in the same field of security tokens and it solves the problem for allowing exercise of various cryptographic capabilities/services under the control of a policy using tokens.

However, Kent in view of Fieres does not teach the message comprising a serialized portion, wherein the serialized portion is serialized based on a key; and key identity information for the key. Kent in view of Fieres does not teach an act of deserializing at least a portion, wherein the serialized portion that is deserialized comprises one or more security tokens created using one or more value types.

De Jong teaches receiving messages through a network, the message comprising a serialized portion [De Jong 11: 0151 --The authenticated digital content request (message) include encrypted security tokens (serialized portion).], wherein the serialized portion is serialized based on a key [De Jong 10: 0140 –Token pool key, or token chain key]; and key identity information for the key [De Jong 10: 0140 –key identifiers for token pool key, or token chain key.]. De Jong teaches receiving messages also comprises an act of deserializing at least a portion of the serialized portion [De Jong 11: 0151 --Upon receiving an authenticated digital content request (message) the content repository uses the chain ID of the received token to determine which token chain to check (chain ID used to initiate deserialization of token chain to check for a particular token.).], wherein the serialized portion that is deserialized comprises one or more security tokens [De Jong 11: 0151 --Token pool, or token chain]created using one or more value types [De Jong 10: 0137 --Token type].
It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Kent in view of Fieres by incorporating encryption of tokens as taught by de Jong. The suggestion/motivation would have been to enhance security by protecting information in a security token related to the packet data payload. De Jong is analogous art because it is in the same field of security tokens, and it solves the problem of enhancing security by protecting token security information.

Kent in view of Fieres and De Jong does not teach the key used to serialize the portion can be accessed at a key provider.

Official notice is taken that it is common and well known in the art to have a technique of accessing keys at a key provider in a scheme known as Key Escrowing.
Kent in view of Fieres, de Jong and a key escrowing scheme for managing keys used to encrypt/decrypt security tokens teaches all the limitations of the above claim.

Regarding claim 2, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 1, wherein the received message includes one or more digital signatures, the method further comprising an act of authenticating at least one of the one or more digital signatures [Fieres 8: 49-55].

Regarding claim 3, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 1, further comprising an act of receiving a message from a sending computer system, the message including an encrypted portion and one or more security tokens [Kent Pg 7, Sec 3.1].

Claim 4 and 5 are cancelled.

Regarding claim 6, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 1, wherein the identified corresponding value type is a custom value type created by the sending computer system or the receiving computer system, and that the receiving and sending computer system can access

[Fieres 14: Table 1 –COS and inclusion of supporting attributes are custom value types.].

Regarding claim 7, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 1, further comprising an act of updating one or more properties of the stored security token that is accessible by the receiving computer system with one or more of the identification information and the custom property [US 6178504 B1, Col 13, Ln 24-32 –Examiner notes COS attributes such as number of usage or expiration time all reading on custom properties.] [US 6178504 B1, Col 19, Ln 12-35 —Examiner notes digital signature (identification information) is evidently updated.]

Regarding claim 8, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 7 further comprising an act of creating a security key when updating the one or more properties of the stored security token [A token chain key is created when a new token chain is being generated because of updated token properties/specifications/parameters. A token pool key is also created when new tokens or token chains or token pools are generated. (de Jong 10: 0140) (de Jong: Fig 20)].

Regarding claim 9, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 1, wherein the identified at least one security

token is serialized in the received message based on a private key that is shared between the sending and receiving computer system [Token pool/chain keys are shared between sending and receiving entities of authenticated digital content requests. (US 2004/0054628 A1, Pg 11, Par 0152)].

Claim 10 is cancelled.

Regarding claim 11, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 1, wherein the one or more security tokens are found in a security header portion of the message [This limitation is part of the Web Services Security communications protocol as taught by de Jong (de Jong 7: Par 0111-0112).].

Regarding claim 12, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method as recited in claim 11, wherein, prior to receiving the message, the at least one identified token is serialized into the security header portion of the message by transforming the at least one identified security token into base 64 encoded data [This type of encoding is built into the Web Services Security communications protocol and such communications protocol is taught by de Jong (de Jong 7: Par 0111-0112).].

Regarding claim 13, Kent in view of Fieres, de Jong and a key escrowing scheme teach the method as recited in claim 12, wherein deserializing comprises an act of converting

data from the identified at least one token from base 64 encoding to a byte array [This type of decoding is built into the Web Services Security communications protocol and such communications protocol is taught by de Jong (de Jong 7: Par 0111-0112).].

Claims 15 and 16 are cancelled.

Regarding claim 34, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method of claim 1, wherein the one or more security tokens are represented in the message by a markup language identifier token, and wherein the at least one identified security token is identified by the markup language identifier [de Jong 10: 0137 --Token Chain ID, offset, token type indicator].

Regarding claim 36, Kent in view of Fieres, de Jong and a key escrowing scheme teaches the method of claim 1, wherein the value type comprises compiled instructions [Fieres 7: 66 – 8: 3 --The cryptographic functions and its other supporting library of programs includes instructions that tell a computer how to read/compute challenge data of a request associated with a specific security token with a corresponding COS. These read on "compiled instructions."].

Regarding claim 17, Kent teaches in a computerized network environment including two or more computer systems sending messages through a network communication protocol [Kent Pg 1, Sec 1, Par 1], a method of sending secure messages using custom

security tokens [Kent Pg 1, Sec 1, Par 2], the method comprising: an act of a sending computer system generating one or more security tokens [Kent Pg 10, Sec 3.3.2] using one or more corresponding value types [Kent Pg 13, Sec 3.4.2 --A security association reads on a "value type."]; an act of encrypting a portion of a message using at least one of the one or more generated security tokens [Kent Pg 10, Sec 3.3.2]; and an act of inserting the at least one generated security token in an outbound token collection [Kent Pg 2, Sec 2].

Kent does not teach wherein the one or more corresponding value type comprise custom program classes including collections of executable instructions for data handling, including instructions that tell a computer system how to read data associated with a specific security token that was created using a specific value type, each token including token data that includes a custom property, wherein the custom property defines one or more of time of day, geographic location, limitations on message access, or limitations on device access, and converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system.

Fieres teaches an act of generating one or more security tokens [Fieres 6: 29-30 -- application certificate reads on tokens] using one or more corresponding value types [Fieres 6: 29-30 --COS reads on value types.], wherein the one or more corresponding value type comprise custom program classes including collections of executable instructions for data handling [Fieres 5: 17-35 --Each type of COS has a particular set of cryptographic functions and supporting library programs for handling data in a

request.], including instructions that tell a computer system how to read data associated with a specific security token that was created using a specific value type [Fieres 7: 66 – 8: 3 --The cryptographic functions and its other supporting library of programs includes instructions that tell a computer how to read/compute challenge data of a request associated with a specific security token with a corresponding COS.], each token including token data that includes a custom property, wherein the custom property defines one or more of time of day, geographic location, limitations on message access, or limitations on device access [Fieres 6: 30 --Application ID of the token reads on a custom property which defines limitations/restrictions of accessing the cryptographic functions of a specific COS reading on "limitations on message access."].
It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Kent by customizing security using one or more corresponding value types as taught by Fieres. The suggestion/motivation for combining would have been to allow for compliance in the distribution and exercise of various cryptographic capabilities under the control of a policy using security tokens. Fieres is analagous art because it is in the same field of security tokens and it solves the problem for allowing exercise of various cryptographic capabilities/services under the control of a policy using tokens.

However, Kent in view of Fieres does not explicitly teach the method further comprising an act of converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system.

De Jong teaches in a computerized network environment including two or more computer systems sending messages through a network communication protocol the act of converting the token data for the outbound token collection using a private key that is accessible by the sending computer system and a receiving computer system [(De Jong 10: 0140) Such a private key is the token pool key, or the token chain key depending on which perspective. Examiner notes that such private keys are securely transported or securely generated as shown by De Jong, Fig. 19 and 24 -- thus are accessible by sending and receiving entities.].

It would have been obvious to one of ordinary skill in the art at the time of invention to combine the digital content access control of de Jong into the invention of Kent in view of Fieres. The suggestion/motivation would have been to have an invention capable of controlling access to the security tokens thereby having an additional layer of restricting access to a message. De Jong is analogous art because it is in the same field of endeavor of controlling access in a digital network through the use of security tokens.

Claim 18 is rejected because it is similar to claim 2.

Regarding claim 19, Kent in view of Fieres, and de Jong teach the method as recited in claim 17, further comprising an act of including private key information in the message [De Jong 10: 0140 –key identifiers for token pool key, or token chain key.],

such that the receiving computer system can access the key from a key provider based on the key information [Official notice is taken that it is common and well known in the art to have a technique of accessing keys at a key provider in a scheme known as Key Escrowing.]

Regarding claim 20, Kent in view of Fieres, and de Jong teach the method as recited in claim 17, wherein the act of converting the token data comprises serializing the token data into base 64 encoding is inherent because this type of encoding is built into the Web Services Security communications protocol and such communications protocol is taught by de Jong [de Jong 7: Par 0111-0112].

Regarding claim 21, Kent in view of Fieres, and de Jong teach the method as recited in claim 17, wherein the at least one generated security token is a custom security token created using a custom value type, and wherein the custom value type is accessible by both the sending and receiving computer systems [Fieres 14: Table 1].

Regarding claim 22, Kent in view of Fieres, and de Jong teach the the method as recited in claim 17, further comprising an act of creating a signature or encryption function based on the included one or more of a custom property, a signature, and an encryption level in the created binary token [Fieres 11: Ln 19-24] [de Jong, Fig 19].

Regarding claims 23 and 24, Kent in view of Fieres, and de Jong teach the method as

recited in claim 17, further comprising an act of including a program language value corresponding with each token that is included in the outbound token collection and wherein the program language value is a Common Language Runtime value [(de Jong 8: Par 0118) du Jong et al. teach "servlet"(s) that can handle the common language infrastructure.].

Claim 25 is cancelled.

Regarding claim 26, Kent in view of Fieres, and de Jong teach the method as recited in claim 17, further comprising an act of assigning the markup language representation of the at least one generated security token a global unique identifier [A global unique identifier is interpreted as a type of identifier known across all platforms or throughout entire network system. Since de Jong's tokens have implementations using URLs, many or all can qualify as a global unique identifier.]

Regarding claim 27 and 28, in view of Fieres, and de Jong teach the method as recited in claim 26, wherein the outbound token collection is a hash table that is keyed by the global unique identifier of the at least one generated security token and wherein the global unique identifier is inserted into a signature or encryption portion of the message [(US 2004/0054628 A1, Pg 10, Par 0140-141) Since the cryptographic process includes a hashing function, the resulting encryption process can be interpreted as a hashing table since tokens taught by de Jong et al. is also organized in a data structure ie. pools

and chains. Many identifiers used by de Jong et al. qualify as the global unique identifier such as the Seed or the last token identifier (since the last token identifier in one embodiment is used to generate the token chain).].

Claim 29 is rejected using references and rationale of claims 17.

Claims 30-31 are cancelled.

Claims 33 is rejected because it is similar matter to claim 24.

Regarding claim 35, the combined invention of Fieres and de Jong teach the method as recited in claim 17, wherein the act of inserting the at least one generated security token in an outbound token collection further comprises: an act of identifying a markup language representation of the at least one generated security token [de Jong 10: 0137 --Token Chain ID, offset, token type indicator], and an act of placing the markup language representation of the at least one generated security token in the outbound token collection [(de Jong 7: starting Par 0140) Such representation is evident in the token pool information.]

2. Claims 14 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kent et al. [NPL 1998], and further in view of Fieres et al. [US 6178504 B1].

Regarding claim 14, Kent teaches in a computerized network environment including two or more computer systems sending messages through a network communication protocol [Kent Pg 1, Sec 1, Par 1], a method of receiving secure messages using custom security tokens [Kent Pg 1, Sec 1, Par 2], the method comprising: an act of at a receiving computer system [Kent Pg 7, Sec 3.1] identifying one or more security tokens in a received message [Kent Pg 12, Sec 3.4.2 --Parsing the packet for processing data extracted from various packet headers reads on "an act of identifying."], from a sending computer system, that has at least a portion that has been encrypted using the one or more security tokens [Kent Pg 10, Sec 3.2.1 --Data payload is encrypted using information from ESP.], and a value type corresponding with each identified security token [Kent Pg 13, Sec 3.4.2 –Security association is a value type.], an act of receiving data from the at least one identified security token into the stored value type that has been matched [Kent Pg 12, Sec 3.4.2 --Parsing the packet, and extracting data for packet processing reads on this limitation.] and an act of decrypting an encrypted portion of the received message using the stored value type [Kent Pg 16, Sec 3.4.5] and accessing the received message based at least in part on the raw data received from the at least one identified security token [Kent Pg 16, Sec 3.4.5 -Information from ESP is used to decrypt data payload of message packet.].

Kent does not teach an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access, wherein the stored value type comprises a custom program classes including a collection of executable instructions for data handling, including instructions that tell a

computer system how to read data associated with a specific security token that was created using the value type. Kent also does not teach wherein the raw data received into the stored value type includes one or more of identification information, and a custom property.

Fieres teaches an act of generating one or more security tokens [Fieres 6: 29-30 --application certificate reads on tokens] using one or more corresponding value types [Fieres 6: 29-30 --COS reads on value types.], an act of matching the identified corresponding value type to a stored value type for a stored security token that the receiving computer system can access, wherein the stored value type comprises a custom program classes including a collection of executable instructions for data handling [Fieres 5: 17-35 --Each type of COS has a particular set of cryptographic functions and supporting library programs for handling data in a request.], including instructions that tell a computer system how to read data associated with a specific security token that was created using a specific value type [Fieres 7: 66 – 8: 3 --The cryptographic functions and its other supporting library of programs includes instructions that tell a computer how to read/compute challenge data of a request associated with a specific security token with a corresponding COS.], and an act of receiving data from the at least one identified security token into the stored value type that has been matched [Fieres 14: 29-55 --COS attributes are extracted and used by the stored COS type program/functions to govern its operation.], wherein the raw data received into the stored value type includes one or more of identification information, and a custom property [Fieres 6: 30 --Application ID of the token reads on a custom property which

defines limitations/restrictions of accessing the cryptographic functions of a specific COS reading on "limitations on message access."].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Kent by customizing security using one or more corresponding value types as taught by Fieres. The suggestion/motivation for combining would have been to allow for compliance in the distribution and exercise of various cryptographic capabilities under the control of a policy using security tokens [Fieres 2: 47-63]. Fieres is analagous art because it is in the same field of security tokens and it solves the problem for allowing exercise of various cryptographic capabilities/services under the control of a policy using tokens.

Regarding claim 32, Kent in view of Fieres teach the method as recited in claim 14, wherein deserializing comprises an act of converting data from the identified at least one token from base 64 encoding to a byte array [Official Notice is taken that it is common and well known in the art to convert data from base 64 encoding to a byte array since this type of decoding is built into the Web Services Security communications protocol].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone

number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan

Examiner. Art Unit 2132

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132